Daniel C. Girard (State Bar No. 114826)
Eric H. Gibbs (State Bar No. 178658)
Adam E. Polk (State Bar No. 273000)
GIRARD GIBBS LLP
601 California Street, Suite 1400
San Francisco, California 94104
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
E-mail: dcg@girardgibbs.com
Email: ehg@girardgibbs.com
E-mail: aep@girardgibbs.com

Attorneys for Individual and Representative Plaintiffs Rhonda Estrella, Sonia Ferezan, John Whittle, and Alan Woyt

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

RHONDA ESTRELLA, SONIA FEREZAN, JOHN WHITTLE, and ALAN WOYT on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

LENOVO (UNITED STATES) INC. and SUPERFISH, INC.,

Defendants.

Case No. 3:15-cv-01044

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Rhonda Estrella, Sonia Ferezan, John Whittle and Alan Woyt, individually and on behalf of a proposed class described below, bring this action for injunctive relief and statutory damages against Defendants Lenovo (United States) Inc. ("Lenovo") and Superfish, Inc. ("Superfish") and allege as follows:

I. SUMMARY OF THE CASE

1. Plaintiffs and Class members are individual purchasers of Lenovo personal computing ("PC") products preloaded with hidden software designed by Superfish that was "buried so deep in the machine's operating system that antivirus scanners couldn't find it."[1]

2. Superfish paid Lenovo "between $200,000 and $250,000"[2] to load its spyware program, VisualDiscovery, onto Lenovo PC users' machines. VisualDiscovery performs advertisement injection services. Superfish is compensated on a 'pay-per-click' basis by its clients to inject banner, pop-up, and similar advertisements when users attempt to access websites. Because Superfish collects a commission every time a user clicks on one of the advertisements it injects, it is in Superfish's economic interest to inject advertisements across as many websites as it can.

3. VisualDiscovery is uniquely invasive in that it has the ability to inject advertisements onto both unencrypted and encrypted websites. So when Lenovo PC users attempt to access either an unencrypted website (www.apple.com for example) or an encrypted website (the password portal to www.bofa.com or www.google.com for example), VisualDiscovery intercepts and scans Plaintiffs and Class members' private data in order to inject targeted advertisements.

4. Because of VisualDiscovery's ability to scan users' sessions on encrypted websites, Lenovo and Superfish expose and continue to expose Lenovo PC users to cyber-attacks that have been described by computer industry and electronic privacy experts as easy to carry out. Attackers need only create a duplicate or "spoof" certificate for the encrypted site (for example

[1] Nicole Perlroth, *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs*, New York Times (March 2, 2015), http://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html?_r=0 (last visited March 2, 2015).

[2] Thomas Fox-Brewster, *Lenovo Only Made up to $250,000 From Nightmare Superfish Deal, Say Sources*, Forbes, http://www.forbes.com/sites/thomasbrewster/2015/02/27/lenovo-got-very-little-from-superfish-deal/ (last visited March 3, 2015).

www.bofa.com's password portal) and Lenovo PC users will automatically be directed to the attacker, who will then harvest the Lenovo PC users' information.

5. In addition to exposing Lenovo PC users to cyber-attacks, VisualDiscovery also actively scans the content of websites that such users access, violating their privacy rights. VisualDiscovery's invasion of Plaintiffs and Class members' privacy is particularly egregious in light of the fact that VisualDiscovery operates across both unencrypted and encrypted websites. VisualDiscovery therefore has the capability to and does scan sensitive content like the normally encrypted data found on the secure personal banking websites. VisualDiscovery—enabled by Lenovo's preloading of the spyware onto certain of its PCs—thus violates Lenovo PC users' privacy rights and exposes them to severe security risks "for the rather ridiculous purpose of serving advertisements."[3]

6. While both Lenovo and Superfish profited financially by including VisualDiscovery on users' PCs, according to Lenovo's Chief Technology Officer ("CTO") Peter Hortensius, inclusion of the spyware added no value to Lenovo PC users' experiences. To the contrary, Lenovo's choice to include VisualDiscovery spyware and other "bloatware" on certain of its PCs negatively impacted the performance of such PCs, slowing them down and dissipating available memory.

7. On February 20, 2015, the Department of Homeland Security ("DHS") issued an alert warning Lenovo PC users that inclusion of VisualDiscovery spyware exposed them to cyber-attacks, and specifically alerting them that "websites, such as banking and email, can be spoofed without a warning from the browser."[4] Since then, Lenovo has released a series of statements about the Superfish scandal in which it admitted that it intentionally installed the software without adequate quality control resulting in harm to its substantial consumer base. Lenovo labeled the Superfish threat on its laptops as "high," its most severe rating, stopped preloading the spyware "in January," and recently released manual uninstall instructions and a patch.

[3] *Lenovo Apologizes After it 'Messed Up' With Tracking Software*, Bloomberg News (Feb. 20, 2015), https://www.internetretailer.com/2015/02/20/lenovo-apologizes-after-it-messed-tracking-software (last visited March 1, 2015).

[4] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*, United States Computer Emergency Readiness Team (Feb. 20, 2015), https://www.us-cert.gov/ncas/alerts/TA15-051A (last visited Feb. 27, 2015).

8. The media, including technology industry publications have uniformly criticized Lenovo's course of conduct as a "catastrophe,"[5] "[r]eckless, careless, and appalling,"[6] "astoundingly stupid,"[7] "horrifically dangerous,"[8] and, "one of the biggest mistakes in [Lenovo's] history."[9] Regarding Lenovo's decision to include VisualDiscovery spyware on its PCs, one security researcher wrote that Lenovo's conduct is "quite possibly the single worst thing I have seen a manufacturer do to its customer base."[10]

9. Lenovo and Superfish have been unjustly enriched by their illegal conduct. Plaintiffs and the Class of Lenovo PC users have been harmed by Lenovo and Superfish in at least three ways: (1) Lenovo damaged PC performance by deciding to preload VisualDiscovery and other bloatware; (2) Defendants violated Plaintiffs and Class members' privacy rights by intercepting and scanning private information without their permission, including the content of encrypted email or banking websites; and, (3) Defendants exposed Plaintiffs and Class members to severe security risks because VisualDiscovery created a vulnerability that has allowed cyber-attackers and criminals to easily access and steal such private information. Defendants engaged in this harmful conduct in order to boost their revenues.

10. Plaintiffs and Class members did not agree to Superfish's interception and scanning of any of their private content. Plaintiffs and Class members specifically did not consent to

[5] Joseph Bonneau, et al., *Lenovo Is Breaking HTTPS Security on its Recent Laptops*, Electronic Frontier Foundation (Feb. 19, 2015), https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops (last visited Feb. 27, 2015).

[6] David Auerbach, *You Had One Job, Lenovo*, Slate (Feb. 20, 2015), http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html (last visited Feb. 27, 2015).

[7] Mike Masnick, *Lenovo In Denial: Insists There's No Security Problem With Superfish—Which is Very, Very Wrong*, Tech Dirt (Feb. 19, 2015), https://www.techdirt.com/articles/20150219/10124430071/big-lenono-lenovo-massively-compromises-customers-security-brushes-it-off-as-no-biggie.shtml (last visited, Feb. 27, 2015).

[8] Ellie Zolfagharifard, *Are You Under Threat from a Superfish Attack? Lenovo PCs May Have Adware—and a "Horrifically Dangerous" Security Flaw*, Daily Mail (Feb. 20, 2015), http://www.dailymail.co.uk/sciencetech/article-2960608/Are-threat-Superfish-attack-Lenovo-PCs-adware-horrifically-dangerous-security-flaw.html.

[9] Thomas Fox-Brewster, *How Lenovo's Superfish 'Malware' Works and What You Can do to Kill It*, Forbes (Feb. 19, 2015), http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-need-to-know/ (last visited Feb. 27, 2015).

[10] Marc Rogers, *Lenovo Installs Adware on Customer Laptops and Compromises All SSL*, Marc's Security Ramblings (Feb. 19, 2015), http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/ (last visited March 1, 2015).

VisualDiscovery's access to content contained on encrypted websites. Defendants failed to disclose that the VisualDiscovery Spyware would inject advertisements across both encrypted and unencrypted websites exposing private information like banking and email credentials—and the content contained on such websites once accessed—to scanning by VisualDiscovery and to cyber-attack by malicious actors.

11. Plaintiffs seek disgorgement, injunctive relief, declaratory relief, and actual, statutory, and exemplary damages on behalf of themselves and a proposed class of other Lenovo PC users whose PCs were intentionally infected with VisualDiscovery spyware designed by Superfish.

II. PARTIES

12. Plaintiff Rhonda Estrella is a resident of the State of California. She owns a Lenovo Yoga 2 Pro that was preloaded with VisualDiscovery spyware. She purchased the Lenovo PC in November 2014.

13. Plaintiff Sonia Ferezan is a resident of the State of Virginia. She owns a Lenovo Yoga 2-11, Model 20428 that was preloaded with VisualDiscovery spyware. She purchased the Lenovo PC in January 2015.

14. Plaintiff John Whittle is a resident of the State of Arizona. He owns a Lenovo PC, Model G50-70 that was preloaded with VisualDiscovery spyware. He purchased the Lenovo PC in October 2014.

15. Plaintiff Alan Woyt is a resident of the State of Texas. He owns two Lenovo PCs, a Yoga 14 and a Yoga 2-11 that were both preloaded with VisualDiscovery spyware. He purchased both of the Lenovo PCs on December 1, 2014 at Best Buy.

16. On numerous occasions during the proposed class period, Plaintiffs accessed both encrypted and unencrypted domains, including www.wellsfargo.com, www.shellfcu.org (Shell Federal Credit Union), and various other bank and credit card websites. Superfish intercepted and scanned Plaintiffs' personal and private information over the course of injecting advertisements into the websites Plaintiffs accessed, exposing their personal and private information to cyber-attack in the process. Plaintiffs did not consent to Superfish's conduct.

17. Defendant Lenovo (United States) Inc. is a Delaware corporation with corporate headquarters at 1009 Think Place, Morrisville, North Carolina, 27560-9002 and a California Regional Office and Research and Product Development Center in this District at 602 Charcot Avenue, San Jose, CA 95131. Lenovo is the American subsidiary of Lenovo Group Limited, a Chinese corporation with corporate headquarters at No. 6 Chuang Ye Road, Shangdi Information Industry Base, Haidian District, Beijing, China. Lenovo researches, manufactures, and sells personal computers, business computers, smartphones, tablets, servers, computer hardware, IT management software, televisions, and wearable electronic devices. Since acquiring IBM's personal computer business in 2005, Lenovo has grown to be the largest PC vendor in the world with approximately 19.9% market share as of the fourth quarter of 2014. For its fiscal year 2013/2014, Lenovo had nearly $39 billion in revenue, 79% of which was derived from the sale of laptop and desktop computers. Lenovo does a substantial amount of business in California. Its computers are sold by retailers in 264 California cities. In the cities of Los Angeles, San Francisco, San Jose, and San Diego alone, Lenovo offers its computers through 61 separate retailers.

18. Defendant Superfish, Inc. is a privately held Delaware corporation with corporate headquarters in this District, at 2595 E. Bayshore Road, #150, Palo Alto, CA 94303. Superfish also maintains offices in Israel at Efal 25, POB 3787, Petach Tikva, 4951125. Superfish is a software development company that advertises itself as delivering "the true promise of visual search" through "patented image-to-image search technology [that] analyzes images from every angle and perspective."[11] Superfish produces software applications that consumers can choose to download and spyware like VisualDiscovery that is preloaded onto PCs and hidden from PC users. According to one report, as of October 2014, Superfish's revenue from affiliate advertising was "on track to land between $45 million and $50 million for [2014], up from $2 million in 2011."[12]

[11] *Making Visual Search an Everyday Reality*, Superfish, http://www.home.superfish.com/ (last visited Feb. 27, 2015).

[12] Patrick Hoge, *Superfish Dives Deep Into Visual Search*, San Francisco Business Times (Oct. 24, 2014), http://www.bizjournals.com/sanfrancisco/feature/fast-100-superfish-dives-deep-into-visual-search.html?page=all (last visited Feb. 27, 2015).

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act, 28 USC § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different than Defendants' states of citizenship, the amount in controversy exceeds $5 million, and the proposed class includes in excess of 100 members.

20. This Court also has subject matter jurisdiction over the federal claims in this action pursuant to 28 USC § 1331.

21. This Court also has subject matter jurisdiction over the state law claims in this action pursuant to 28 USC § 1367(a) because they are so related to the federal claims that they form part of the same case or controversy under Article III of the U.S. Constitution.

22. This Court has personal jurisdiction over Defendant Superfish because Superfish is headquartered in California and much of the relevant conduct occurred in California.

23. This Court also has personal jurisdiction over Defendants because they conduct substantial business in this District.

24. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants reside in this district and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred here.

IV. FACTUAL ALLEGATIONS

Lenovo and the Personal Computing Industry

25. As the largest PC vendor in the world, Lenovo sells hundreds of millions of units per year. In the United States alone, for the fiscal quarter ended December 31, 2014, Lenovo reported earning $4.3 billion in revenue and holding 11.1% of the PC market. Lenovo sold 16 million Windows computers in the fourth quarter of 2014.

26. Lenovo and other PC manufacturers have recently been slashing prices on their hardware in a competitive "race to the bottom."[13] For example, some of the Lenovo models at issue

[13] Brad Chacos, *Bloatware: Why Computer Makers Fill Your PC With Junk, and How to Get Rid of It*, PCWorld (Feb. 26, 2015), http://www.pcworld.com/article/2889292/bloatware-why-computer-makers-fill-your-pc-with-junk-and-how-to-get-rid-of-it.html (last visited March 1, 2015).

in this case retail for just $349.95, a price point below even the "historically low levels" of $410-$430 per unit reported in October 2014. PC vendors make "little to no money on such slim margins."[14]

27. According to a report by Forbes, Superfish paid Lenovo "between $200,000 and $250,000" to preload its VisualDiscovery spyware onto its PC users' machines—"a paltry sum given the massive earnings at the Chinese giant . . . ."[15]

28. In an effort to offset its discounted prices for hardware and increase revenue, Lenovo accepts payment from software developers like Superfish to preload its PCs with the developers' programs. Known as "bloatware" or "crapware," the preloaded software often loads at startup, wastes memory, creates potential conflicts with other applications, and slows down performance. To quantify the effect of preloaded bloatware on performance, Microsoft's "clean" version of Windows—Microsoft Signature—outperformed PCs without Signature by starting up 39.6% faster, entering sleep mode 23.1% faster, and resuming 51.3% faster. Furthermore, independent from the general negative effects of bloatware on PC performance, VisualDiscovery—the Superfish-designed spyware at issue in this case—caused "buggy" web experiences for Plaintiffs and Class members. Despite these negative effects on performance, Lenovo continues to preload software onto its PC users machine because—as was recently reported by Forbes—there's a lot of money to be earned by simply bundling extra 'crapware' onto people's PCs."[16]

Superfish, Visual Search Technology, and Lenovo's Decision to Preload Superfish VisualDiscovery Spyware on Certain of Its PCs

29. According to the DHS's Computer Emergency Readiness Team, starting in at least September 2014, Lenovo preloaded VisualDiscovery spyware as part of its bloatware preinstallation on certain of its PCs.

30. According to a press release issued by Lenovo, the following PC models were infected with VisualDiscovery spyware:

---

[14] *Id.*

[15] *Lenovo Only Made Up To $250,000 From Nightmare Superfish Deal, Say Sources.*

[16] Thomas Fox-Brewster, *Superfish: A History of Malware Complaints and International Surveillance*, Forbes (Feb. 19, 2015), http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-history-of-malware-and-surveillance/ (last visited Feb. 27, 2015).

- **E-Series:** E10-30
- **Flex-Series:** Flex 2 14, Flex 2 15, Flex 2 14D, Flex 2 15D, Flex 2 Pro, Flex 10
- **G-Series:** G410, G510, G710, G40-30, G40-45, G40-70, G40-80, G50-50, G50-45, G50-70, G50-80, G50-80Touch
- **Lenovo Edge 15**
- **Miix-Series:** Miix2 – 8, Miix2 – 10, Miix2 – 11, Miix3 – 1030
- **S-Series:** S310, S410, S415, S415 Touch, S435, S20-30, S20-30 Touch, S40-70
- **U-Series:** U330P, U430P, U330 Touch, U430 Touch, U530 Touch
- **Y-Series:** Y430P, Y40-70, Y40-80, Y50-70, Y70-70
- **Yoga Series:** Yoga2-11, Yoga2-13, Yoga2Pro-13, Yoga3Pro
- **Z-Series:** Z40-70, Z40-75, Z50-70, Z50-75, Z70-80.

31. VisualDiscovery is advertisement injection ("ad-injection") spyware designed and sold by Superfish, a privately held software development company with offices in Palo Alto, California and Israel. Superfish was recently ranked 64th on Forbes' list of the most promising American companies of 2015, reporting revenues of $38 million. According to Forbes, "[i]t pays to be invasive these days."[17] In 2013, Superfish's revenue reached $35.3 million—an increase of 26,000 percent over the previous three years.[18]

32. Superfish was co-founded by Adi Pinhas and Michael Chertok—two "veterans of the video surveillance industry"[19] with a history questionable privacy practices. In 1999, they founded Vigilant Technology which "invented digital video recording for the surveillance market" and reports contracts with the United States military's White Sands Missile Range, Paradise Casinos, prisons, and several Israeli government organizations, among others.[20] Before founding Vigilant, Pinhas worked at Verint, an intelligence company where he carried out "signal processing research" in which he would analyze information disseminated through telephone lines. Verint is alleged to have

[17] *Superfish: A History of Malware Complaints and International Surveillance.*

[18] *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs.*

[19] *Id.*

[20] *Superfish: A History of Malware Complaints and International Surveillance.*

tapped Verizon's communications lines and was supposedly working with the National Security Agency in doing so.

33. In 2006, Pinhas and Chertok founded "Link-It"—a start-up designed to be a "visual search" engine for images "[m]uch in the same way that Google is a search engine for text, Siri for voice, and music discovery apps like Shazam help people match songs they hear on the radio to an artist and song title . . . ."[21] In 2009, Pinhas and Chertok renamed Link-It Superfish.

34. Superfish has been subject to criticism since it was known as Link-It in 2006. One program it designed, "WindowShopper"—like VisualDiscovery—was preloaded onto users machines as bloatware. WindowShopper was widely harangued as unwanted malware that "bombarded users with annoying ads and diverted them to websites they didn't want to visit."[22]

35. One of the cores of Superfish's business is its visual search technology. Superfish employs 12 Ph.Ds. and owns 10 patents related to software that trawls the internet and uses mathematical models to catalog, analyze, and match images of consumer products to the exact consumer products offered by certain retailers. The technology has been very successful—Superfish had advertising deals with "some of the biggest names in e-commerce—Amazon, eBay and Alibaba among them."[23]

36. In 2014, Superfish—looking for new streams of income—landed a deal with Lenovo to install its VisualDiscovery spyware on Lenovo's PCs. Superfish's executives report that they approached Lenovo and said that VisualDiscovery could "'improve . . . consumer experience' by serving more relevant ads."[24]

37. According to industry experts, typically, when software is preloaded onto a PC, the hardware maker—here, Lenovo—is paid a fee per machine.[25] But here, in addition to a reported

[21] *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs*.

[22] *Microsoft, Lenovo Scramble to Protect Users From Superfish Security Flaw*, CBS News (Feb. 22, 2015), http://www.cbsnews.com/news/microsoft-lenovo-superfish-security-flaw/ (last visited March 1, 2015).

[23] *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs*.

[24] *Id.*

[25] *Id.*

$200,000 to $250,000 up front fee, experts "suspect Lenovo was also paid a cut of any Superfish ad revenue generated on their PCs."[26] Thus, Lenovo and Superfish's economic interests were aligned in that the entities would generate more profits: (1) the more machines VisualDiscovery was installed on; and, (2) the more websites—encrypted and unencrypted—on which VisualDiscovery operated.

38. In addition to reaping profits directly from VisualDiscovery, Lenovo also hid the spyware on Plaintiffs and Class members' PCs: "Peter Horne, who has worked in the financial services technology industry for 25 years, noticed that the adware was buried so deep in the machine's operating system that antivirus scanners couldn't find it."[27]

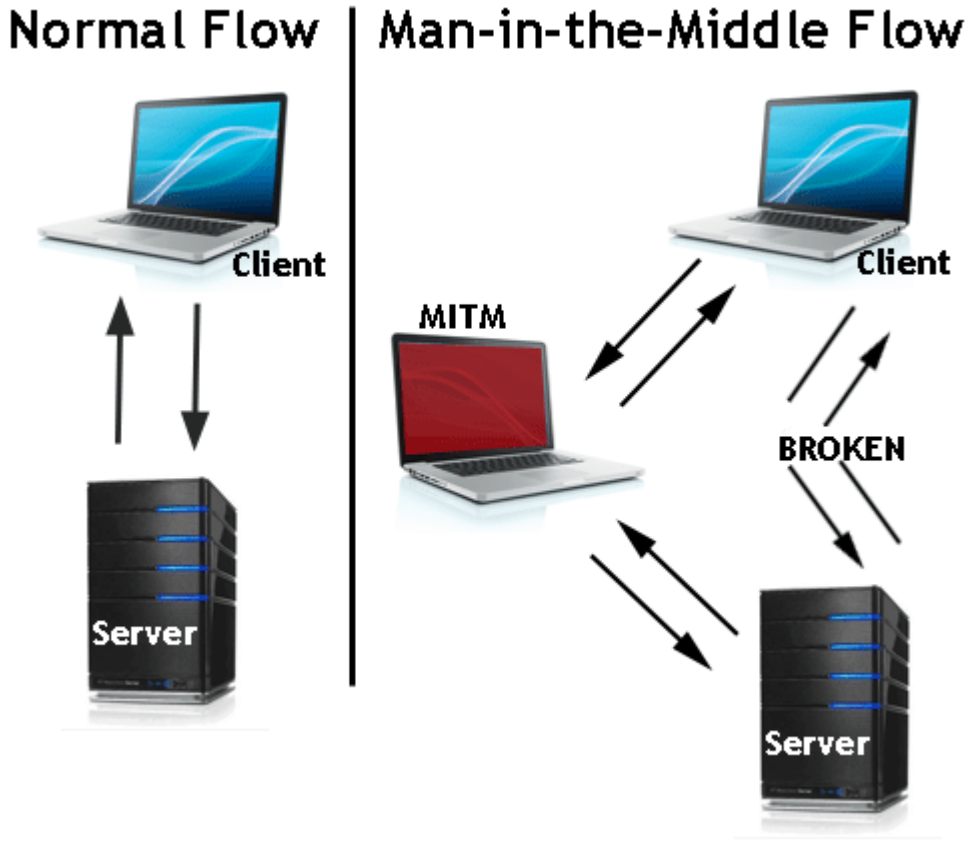
The Technology Underlying Advertisement Injection Spyware and the Unique Dangers VisualDiscovery Presents

39. VisualDiscovery is third party ad-injection spyware—bloatware designed to intercept and scan users' web traffic to inject unauthorized targeted advertisements. The software inserts advertisements into websites without the domain-owner's permission. VisualDiscovery spyware acts as a "man-in-the-middle" between the user and the server for the website the user is attempting to access. Through the man-in-the-middle process VisualDiscovery and other ad-injection spyware forcibly displaces the contents of a website, overlaying or "injecting" it with its own. For example, the following image shows an H&R Block advertisement being injected onto www.apple.com:

[26] *Id.*

[27] *Id.*

40. A man-in-the-middle attack occurs where an actor inserts himself "into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send each other."[28] Man-in-the-middle attacks allow Superfish and other malicious actors—including cyber-attackers—to intercept, scan, send and receive data meant for someone else, or not meant to be sent at all, without outside parties like Plaintiffs and Class members knowing until it is too late. The following image illustrates the difference between a normal connection between a PC user and a certain domain, and a connection with the presence of a man-in-the-middle attacker like VisualDiscovery:



41. When installed, using man-in-the-middle attacks, VisualDiscovery actively scans the content of websites that Lenovo PC users access for retail products and injects advertising banners, pop-up advertisements and in-text ads that offer similar products stating that they are "brought to you

[28] Neil Dupal, *Man in the Middle Attack*, Veracode, http://www.veracode.com/security/man-middle-attack (last visited March 2, 2015).

by 'Superfish.'" According to one analysis of the VisualDiscovery spyware, the advertisements also promote installation of additional questionable content "including web browser toolbars, optimization utilities and other products."[29]

42. Superfish deploys man-in-the-middle attacks to make money. It generates pay-per-click revenue from the companies promoting the injected advertisements—in other words, it gets a commission from its sponsors with every click from users. It is thus in Superfish's economic interest to disseminate its injected advertisements across as many domains as possible, whether encrypted or unencrypted.

43. Typically, ad-injection spyware only intercepts and scans web traffic to unencrypted websites like "www.apple.com" denoted by "HTTP" (Hyper Text Transfer Protocol). The spyware then injects advertisements onto the website the user targets. This is true because normally, ad injection spyware sees encrypted data on websites like www.bofa.com's password portal or Plaintiffs and Class members' password protected personal banking websites as an encrypted and inaccessible jumble of text. Encrypted websites are denoted by "HTTPS" (Hyper Text Transfer Protocol Secure).

44. According to the DHS, VisualDiscovery is uniquely invasive in that it intercepts, scans, and analyzes users' web traffic to provide targeted advertisements over encrypted, HTTPS connections. Because ad-injection spyware usually intercepts traffic before it arrives at a user's browser, under normal circumstances, encrypted connections would remain encrypted. VisualDiscovery operates differently—"[i]nstead of treating your HTTPS traffic as sacrosanct and leaving it alone" the spyware circumvents the protections of encrypted websites by installing a root certificate authority that intercepts and scans browser-based encrypted traffic, decrypts it, and re-encrypts it to the user's browser using an application—conduct described by the DHS as a "classic man-in-the middle attack."[30] Moreover, because VisualDiscovery intercepts and scans users' sessions on encrypted websites, "the browser will not display any warnings that the traffic is being tampered with" and users will have difficulty detecting the presence of the spyware.

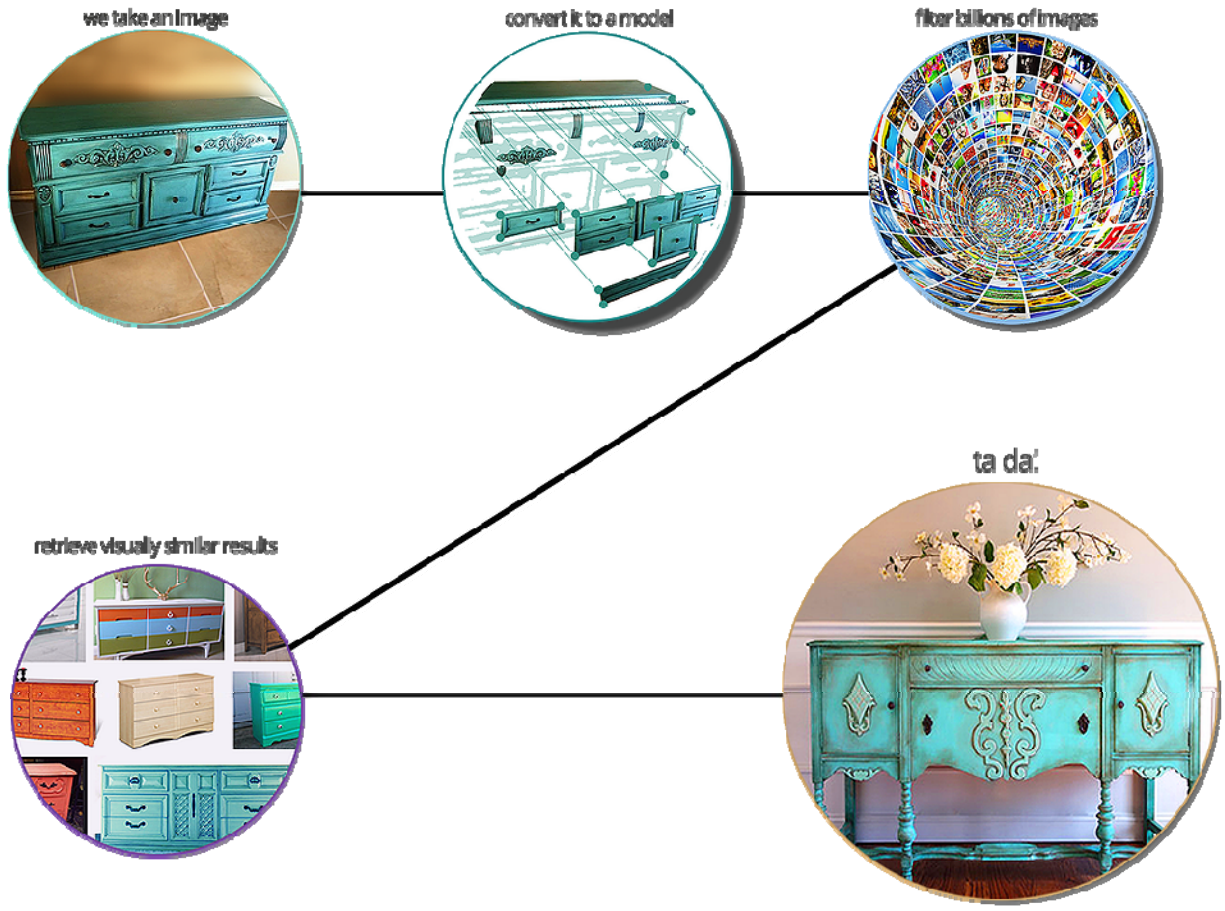
---

[29] *Remove "Superfish" adware (Virus Removal Guide)*, Malware Tips (Oct. 7, 2014), http://malwaretips.com/blogs/superfish-removal/ (last visited March 2, 2015).

[30] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*.

Defendants' Violated Plaintiffs and Class Members' Privacy Rights

45. VisualDiscovery's ability to inject advertisements onto secure, encrypted HTTPS websites violated Plaintiffs and Class members' privacy rights because the software performed scans of the content of the encrypted websites Plaintiffs and Class members accessed. As the following image taken from Superfish's website demonstrates, there are five steps to Superfish's technology: (1) "we take an image;" (2) "convert it to a model;" (3) "filter billions of images;" (4) retrieve visually similar results; and, (5) "ta da!"[31]



In order to complete steps 2 ("convert it to a model") and 3 ("filter billions of images"), Superfish necessarily must first scan and analyze the content of the websites users access.

[31] Technology, Superfish, http://www.home.superfish.com/#!technology/c1bxh (last visited March 2, 2015).

46. Plaintiffs and Class members did not consent to Superfish's scanning the content of data they accessed on either unencrypted (HTTP) or encrypted (HTTPS) websites. This unwarranted violation of Plaintiffs and Class members' privacy rights is more extreme in light of the sensitive content displayed on encrypted websites.

Defendants Exposed Plaintiffs and Class Members to "Horrific" Security Risks

47. Defendants' conduct also exposed Plaintiffs and Class members to security risks one analyst called "horrifically dangerous."[32] By intercepting and scanning users' web traffic over encrypted HTTPS connections, VisualDiscovery creates a technological vulnerability that attackers can easily take advantage of to steal users' private information like banking and email credentials and the content on encrypted websites through a process called "spoofing." Spoofing is a cyber-attack in which a malicious party impersonates another device or user on a network in order to "launch attacks against network hosts, steal data, spread malware or bypass access controls."[33]

48. Users of products infected with VisualDiscovery spyware like Plaintiffs and Class members are particularly vulnerable to spoofing because the spyware combines a technique known as "keybridging" or man-in-the-middle with Secured Sockets Layer ("SSL") certificate manipulation to decrypt the content on otherwise secure, encrypted sites.[34]

49. Information contained on HTTPS websites is generally protected via public/private key encryption. Public/private key encryption uses two different keys at once—a public key and a private key. The public key is used for encryption and the private key is used for decryption. Both keys are kept by the web server that runs the website a user is seeking to access. When a user wants to send confidential information to a website, the user's web browser will access the web server's digital certificate and obtain its public key to encrypt the data and initiate the secure session. Web servers are the only entities with access to private keys, and only web servers can decrypt encrypted information. By deploying keybridging technology to act as a "man-in-the-middle" and by engaging

[32] *Are You Under Threat from a Superfish Attack? Lenovo PCs May Have Adware—and a "Horrifically Dangerous" Security Flaw.*

[33] *Spoofing Attack: IP, DNS & ARP*, Veracode, http://www.veracode.com/security/spoofing-attack (last visited March 2, 2015).

[34] *Lenovo "Superfish" Controversy—What You Need to Know.*

in SSL certificate manipulation, VisualDiscovery gains access to both the public and private keys and decrypts users' incoming and outgoing private information thereby.

50. VisualDiscovery plugs into the portion of users' operating systems that deals with network traffic. So when a user seeks to access a website, the connection is handled directly by VisualDiscovery. Through man-in-the-middle keybridging, when a user seeks to access a website, the user's connection terminates inside VisualDiscovery' filter and VisualDiscovery then completes the connection to the website the user sought to access. Thus Superfish, via VisualDiscovery, connects directly to the website a user seeks to access, acting as a "man-in-the-middle" between the website and the user, and gains the website's public key—which is intended to go to the user—in the process.

51. Under normal circumstances, man-in-the-middle keybridging would only allow ad-injectors to intercept and scan users' attempts to access unencrypted HTTP websites because ad-injectors see HTTPS websites as encrypted. This is true because encrypted websites are secured by SSL technology. When a user seeks to access an encrypted HTTPS website, that user's web browser uses the public key contained in the website's SSL certificate to initiate a secure session by transmitting encrypted data. SSL certificates authenticate the identity of the secure website to browser users and enable encrypted communications. SSL certificates are issued by a group of entities known as trusted Certificate Authorities whose identities are pre-programmed into web-browsers as "trusted advisors" or "trusted root Certification Authorities." "Much like the role of the passport office, the role of the [Certificate Authority] is to validate the certificate holder's identity and to 'sign' the certificate so that it cannot be tampered with."[35] After the SSL certificate holder is validated, the web server will decrypt content using its private key.

52. VisualDiscovery circumvents SSL technology by using software developed by an Israeli company known as Komodia that installs a "self-signed root HTTPS certificate that can

[35] *Understanding Digital Certificates & Secure Sockets Layer*, Entrust (May 2007), available at http://www.entrust.net/ssl-resources/pdf/understanding_ssl.pdf (last visited March 3, 2015).

intercept encrypted traffic for every website a user visits."[36] In other words, Komodia provides a "fake secure sockets layer certificate"[37] with its own private key that allows Superfish to install itself as both the trusted Certificate Authority and the SSL certificate holder for all HTTPS websites accessed via the affected Lenovo PCs. By doing so, Superfish "falsely represents itself as the official website certificate."[38] The HTTPS web server then combines the public key with Superfish's own private key and decrypts the secure content under the mistaken belief that Superfish is a properly vetted SSL certificate holder. In fact, Superfish—acting as a trusted Certificate Authority—simply (and falsely) rubber-stamps itself as approved by a legitimate trusted Certificate Authority. By doing so, Superfish gains access to Plaintiffs and Class members' private information. And "[b]ecause the certificates used by Superfish are signed by the [Certificate Authority] installed by the software, the browser will not display any warnings that the traffic is being tampered with."[39]

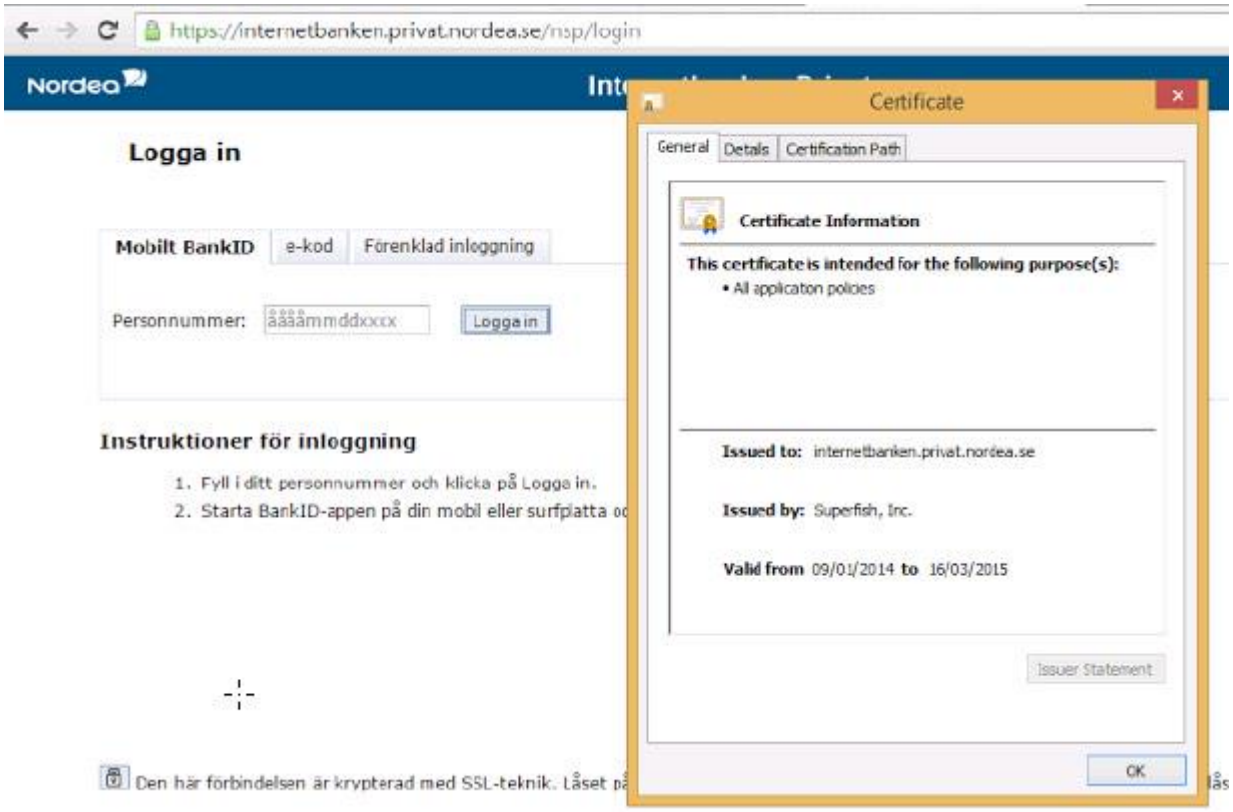
53. The following are screenshots taken from recent analyses of the Superfish scandal that demonstrate Superfish issued self-signed certificates for access to users' secure, encrypted personal banking websites.

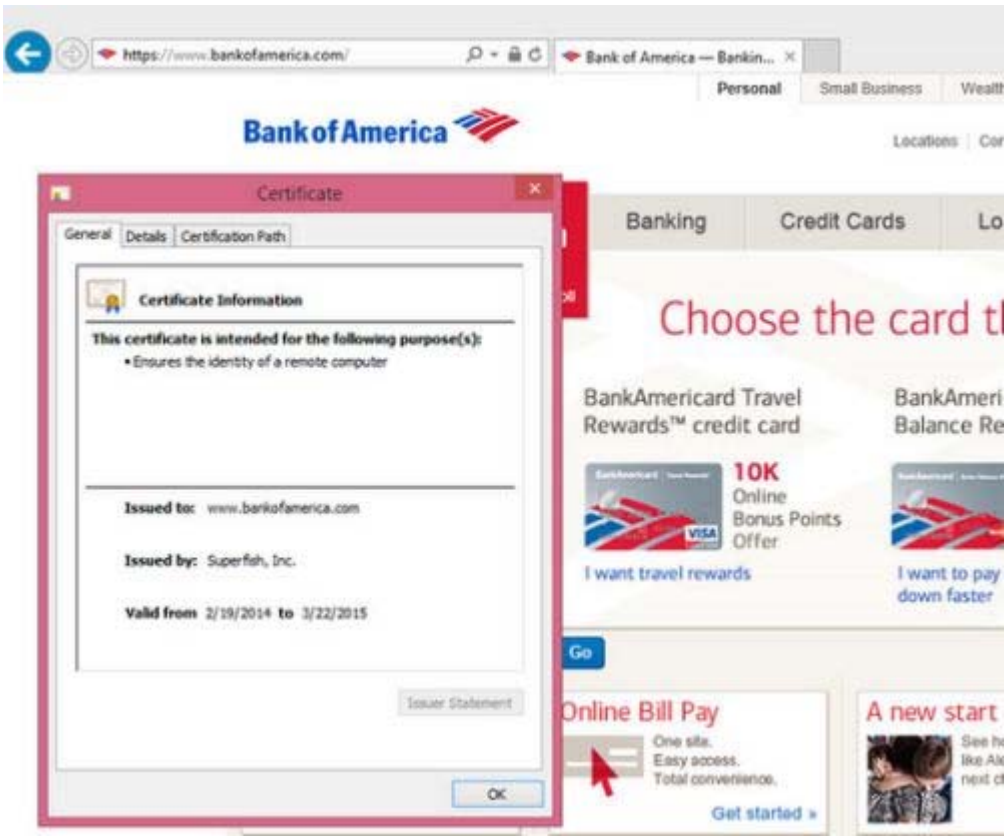
[36] Dan Goodin, *Lenovo PCs Ship With Man-In-The-Middle Adware That Breaks HTTPS Connections*, *ARS Technica* (Feb. 19, 2015), http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/ (last visited March 2, 2015).

[37] Dan Goodin, *"SSL Hijacker" Behind Superfish Debacle Imperils Large Number of Users*, ARS Technica (Feb. 20, 2015), http://arstechnica.com/security/2015/02/ssl-hijacker-behind-superfish-debacle-imperils-big-number-of-users/ (last visited March 2, 2015).

[38] *Id.*

[39] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*.


https://internetbanken.privat.nordea.se/nsp/login
Nordea
Logga in
Mobilt BankID
e-kod
Förenklad inloggning
Personnummer:
åååämmddxxxx
Logga in
Instruktioner för inloggning
1. Fyll i ditt personnummer och klicka på Logga in.
2. Starta BankID-appen på din mobil eller surfplatta
Den här förbindelsen är krypterad med SSL-teknik. Låset
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: internetbanken.privat.nordea.se
Issued by: Superfish, Inc.
Valid from 09/01/2014 to 16/03/2015
Issuer Statement
OK


https://www.bankofamerica.com/
Bank of America — Bankin...
Personal
Small Business
Bank of America
Locations
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: www.bankofamerica.com
Issued by: Superfish, Inc.
Valid from 2/19/2014 to 3/22/2015
Issuer Statement
OK
Banking
Credit Cards
Choose the card t
BankAmericard Travel Rewards™ credit card
10K Online Bonus Points Offer
I want travel rewards
I want to pay down faster
Go
Online Bill Pay
One site. Easy access. Total convenience.
Get started »
A new start

54. According to the Electronic Frontier Foundation ("EFF")—the "leading nonprofit organization defending civil liberties in the digital world"—VisualDiscovery's keybridging and SSL certificate manipulation is "wildly inappropriate" in that it exposes Lenovo PC users to easily executed cyber-attacks. VisualDiscovery allows attackers to create fake domains that users will automatically be redirected to because Komodia handles invalid certificates by altering the part of the certificate that specifies what website the certificate is for—"for example changing www.eff.org to verify fail.eff.org—and then signs the certificate and sends it on" to users' browsers.[40]

55. Normally, where a domain name does not match the website a user is seeking to access, the user will receive a warning. But SSL certificates have a separate field called "Subject Alternative Name" which lists alternative domain names for which the certificate can be used without generating a user warning.[41] Because Superfish self-signs its SSL certificates, even where the domain name listed on an SSL certificate does not match the domain name of the website the user is browsing, the certificate will still be accepted and no warning will be given as long as one of the Subject Alternative Names matches. Accordingly, in order to hijack users' private information, all a cyber-attacker would have to do is "create an invalid certificate with the target domain [www.bofa.com for example] as one of the alternative names, and every" product with VisualDiscovery installed would cause it to be accepted. The "certificate will pass all the browser's checks, and come up smelling like roses."[42] Thus, when the user types his or her credentials into the fake domain, the cyber-attacker—not the secure website—harvests the information. The attacker "doesn't even need to know which Komodia-based product a user has . . . they just have to create an invalid certificate with the target domain as one of the alternative names, and **every** Komodia-based product will cause it to be accepted."[43]

[40] Joseph Bonneau, et al., *Dear Software Vendors: Please Stop Trying to Intercept Your Customer's Encrypted Traffic*, Electronic Frontier Foundation (Feb. 25, 2015), https://www.eff.org/deeplinks/2015/02/dear-software-vendors-please-stop-trying-intercept-your-customers-encrypted (last visited Feb. 27, 2015).

[41] *Id.*

[42] *Id.*

[43] *Id.* (emphasis in original).

56. The DHS similarly warned: "[s]ince the private key can easily be recovered from the Superfish software, an attacker can generate a certificate for any website that will be trusted by a system with the Superfish software installed. This means websites, such as banking and email, can be spoofed without a warning from the browser."[44]

57. According to the EFF, attackers have been taking advantage of users in exactly this manner on a widespread basis:

> [w]e searched the Decentralized SSL Observatory for examples of certificates that Komodia should have rejected, but which it ended up causing browsers to accept, and found over 1600 entries. Affected domains include sensitive websites like Google (including www.google.com, accounts.google.com, and checkout.google.com), Yahoo (including login.yahoo.com), Bing, Windows Live Mail, Amazon, eBay (including checkout.payments.ebay.com), Twitter, Netflix, Mozilla's Add-Ons website, www.gpg4win.org, several banking websites (including mint.com and domains from HSBC and Wells Fargo), several insurance websites, the Decentralized SSL Observatory itself, and ever superfish.com.[45]

58. Based on these findings, the EFF found that it is possible that Komodia—the software on which VisualDiscovery is based:

> enabled real MitM attacks which gave attackers access to people's email, search histories, social media accounts, e-commerce accounts, bank accounts, and even the ability to install malicious software that could permanently compromise a user's browser or read the encryption key. [46]

59. Superfish's choice to run the VisualDiscovery software on a software library developed by Komodia greatly increased Plaintiffs and Class members' exposure to cyber-attack. Komodia "proudly markets HTTPS-decrypting and interception software that's used by more than 100 clients, including Fortune 500 companies."[47] According to a recent promotional video, Komodia—which advertises itself as an "SSL hijacker"—boasts "[w]ith a simple-to-control interface,

---

[44] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*.

[45] *Id.*

[46] *Id.*

[47] *"SSL Hijacker" Behind Superfish Debacle Imperils Large Number of Users*.

you can intercept website traffic and network applications from any program in any program language."[48]

60. Though the "fake [SSL] certificate found on Lenovo machines preinstalled with Superfish . . . was bundled with a password-protected private encryption key . . . the measure was laughably easy to bypass, since it took Errata Security CEO Rob Graham just three hours to discover that **the password was—you guessed it—'Komodia.**'"[49] According to one analyst, once cyber-attackers "do (or did)" figure out that the password to Komodia's false SSL certificate is Komodia, such cyber-attackers:

> will have a master private key that will decrypt traffic travelling between the user and any HTTPS-connected **website** on the Internet. When in a position to monitor the connections between end users and the websites they browse—say, at a coffee shop—these bad actors can use the certificate to intercept and decrypt encrypted traffic flowing both ways.[50]

61. Robert Graham—a security researcher—tested how easy it is to carry out a cyber-attack on an affected Lenovo PC, demonstrating that the risk is "more than merely theoretical."[51] Graham extracted the SSL certificate from VisualDiscovery and "cracked the password ('Komodia') that encrypted it" using "simple reversing."[52] Graham stated that "[a]rmed with the password . . . I can now . . . man-in-the-middle people with Lenovo desktops (in theory, I haven't tried it yet)."[53]

62. Neither Lenovo nor Superfish disclosed that its ad-injection services operated on both encrypted HTTP and unencrypted HTTPS domains exposing Plaintiffs and Class members to cyber-attack. Plaintiffs and Class members thus had no meaningful opportunity to consent to Defendants' conduct.

---

[48] *Id.*

[49] *Id.* (emphasis added).

[50] *Id.*

[51] Seth Rosenblatt, *Lenovo's Superfish Security SNAFU Blows Up in its Face*, CNET (Feb. 20, 2015), http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/ (last visited Feb. 27, 2015).

[52] Robert Graham, *Extracting the Superfish Certificate*, Errata Security (Feb. 19, 2015), http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html#more (last visited March 3, 2015).

[53] *Id.*

Discovery of the Superfish Scandal and Defendants' Evolving Reactions

63. As reported by the New York Times, in early January Peter Horne—a "25-year veteran of the financial services technology industry"—discovered VisualDiscovery on a new Lenovo Yoga 2 Notepad computer he purchased in Sydney Australia.[54] Though Mr. Horne ran the preloaded McAfee antivirus software and antivirus software designed by Trend Micro—neither isolated VisualDiscovery. After discovering the spyware on his PC, Mr. Horne went to test Lenovo demonstration PCs at retailers in New York, Boston, Sydney, and Perth and detected VisualDiscovery on other Lenovo PC models. Mr. Horne noted that Lenovo "had placed the adware [at] a very low-level part of the operating system . . . . If they can do that, they can do anything."[55]

64. Lenovo has been aware of the problems associated with VisualDiscovery since at least Jan. 21, 2015, when "an apoplectic user posted a detailed description of Superfish and its problems" and requested a refund.[56] His post went unanswered for a month, giving cyber-attackers time to exploit the vulnerability VisualDiscovery created. When Lenovo did respond, it did so by "claim[ing] Superfish had been disabled and posed no threat, even though merely uninstalling Superfish *doesn't remove the evil root certificate*."[57] In an interview with the Wall Street Journal, Lenovo's CTO "vaguely acknowledged a problem and then brushed it away: 'We're not trying to get into an argument with the security guys. They're dealing with theoretical concerns. We have no insight that anything nefarious has occurred.'"[58] According to one technology industry writer, this is akin to a statement that "yes, your security company left your house unlocked, but we just don't know if anyone walked right in."[59]

[54] Nicole Perlroth, *Researcher Discovers Superfish Spyware Installed on Lenovo PCs*, New York Times (Feb. 19, 2015), http://bits.blogs.nytimes.com/2015/02/19/researcher-discovers-superfish-spyware-installed-on-lenovo-pcs/ (last visited March 3, 2015).

[55] *Id.*

[56] *You Had One Job Lenovo*.

[57] *Id.* (emphasis in original).

[58] *Id.*

[59] *Id.*

65. As news of the dangers presented by VisualDiscovery started to break, Lenovo initially stood behind its decision to preload the spyware on Lenovo PC users' machines. It issued a statement on Thursday, February 19, 2015, stating that it installed the spyware "[i]n our effort to enhance our user experience" by improving "the shopping experience using [Superfish's] visual discovery techniques."[60] Lenovo explained that it included VisualDiscovery "to help customers potentially discover interesting products while shopping."[61] Lenovo added that it had received certain customer complaints about the software, apologized "for causing any concern to any users for any reason," and said that it "stopped the preloads in January."[62]

66. On February 20, 2015, the DHS issued its alert warning Lenovo PC users that inclusion of VisualDiscovery spyware created a "critical vulnerability that exposed them to cyber-attack, explaining:

> In order to intercept encrypted connections (those using HTTPS), [VisualDiscovery] installs a trusted root CA certificate for Superfish. All browser-based encrypted traffic to the Internet is intercepted, decrypted, and re-encrypted to the user's browser by the application—a classic man-in-the-middle attack. . . . [W]ebsites, such as banking and email, can be spoofed without a warning from the browser.[63]

67. Lenovo then released a series of statements about the Superfish scandal in which it admitted: (1) that it installed VisualDiscovery on certain of its PCs intentionally; (2) that the software added no value to the Lenovo PC user experience; (3) that it was not aware of the security threat VisualDiscovery presented to Lenovo PC users until after Peter Horne and the New York Times reported on the story; and, (4) that VisualDiscovery did in fact expose Lenovo PC users to vulnerabilities:

- "Beginning in September 2014, **we made a decision** to ship some of our consumer notebooks with Superfish."[64]

[60] *Lenovo Statement on Superfish*, Lenovo (Feb. 19, 2015), http://news.lenovo.com/article_display.cfm?article_id=1929 (last visited March 3, 2015).

[61] *Researcher Discovers Superfish Spyware Installed on Lenovo PCs.*

[62] *Lenovo Statement on Superfish.*

[63] *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing.*

- "This software frustrated some of our users **without adding value to the experience** . . . ."[65]
- On February 20, 2015: "**we did not know about this potential security vulnerability until yesterday. Now we are focused on fixing it.**"[66]
- [W]e are determined to make this situation better . . . and prevent . . . the kind of vulnerabilities **that were exposed in the last week**."[67]

68. On February 20, 2015, Lenovo issued an "updated" statement on Superfish, apologizing for the security vulnerability created by VisualDiscovery.[68] The same day, Peter Hortensius—Lenovo's CTO admitted, "**we messed up badly**" and again cited the justification "[t]he intent was to supplement the shopping experience."[69]

69. In an interview with InfoWorld, Mark Cohen—Lenovo's vice president in charge of the Company's "Windows Ecosystem" explained that Lenovo had screened VisualDiscovery in September 2014 and detected certain features that "abused SSL connections."[70] According to Cohen, Lenovo asked that Superfish remove the abusive features, Superfish said it did, and then Lenovo "felt confident to ship [the] feature as a value-add rather than as adware."[71] So Lenovo knew about the danger presented to its PC users before VisualDiscovery was preloaded and shipped to the public,

[64] *Superfish Update—An Open Letter from Lenovo CTO Peter Hortensius*, Lenovo (Feb. 23, 2015), http://news.lenovo.com/article_display.cfm?article_id=1932 (last visited March 3, 2015) (emphasis added).

[65] *Id.* (emphasis added).

[66] *Updated Lenovo Statement on Superfish*, Lenovo (Feb. 20, 2015), http://news.lenovo.com/article_display.cfm?article_id=1931 (last visited Feb. 27, 2015) (emphasis added).

[67] *Superfish Update—An Open Letter from Lenovo CTO Peter Hortensius* (emphasis added).

[68] *Id.*

[69] Seth Rosenblatt, *Lenovo's Superfish Security SNAFU Blows Up in its Face* (emphasis added).

[70] Simon Phipps, *Lenovo: "We Were As Surprised As You,"* InfoWorld (Feb. 201, 2015), http://www.infoworld.com/article/2886959/laptop-computers/are-you-buying-risk-along-with-your-laptop.html (last visited March 3, 2015).

[71] *Id.*

asked for a fix, but never checked it prior to shipping, which means "Lenovo's protocols for validating preinstalled third-party software are somewhere between broken and nonexistent."[72]

70. Lenovo has since labeled the threat presented by VisualDiscovery "high," its most severe rating and has provided ways for users to uninstall the malicious spyware.

71. Superfish has been less conciliatory. In a statement e-mailed to ARS Technica attributed to Superfish CEO Adi Pinhas, Superfish said that VisualDiscovery "poses no threat to end users" but made no mention of SSL technology, HTTPS, or any other form of encryption.[73] Superfish echoed Lenovo's early statements, asserting that the Software was preloaded onto certain Lenovo PCs "to enhance the online shopping experience for Lenovo customers."[74] But even Superfish admitted that VisualDiscovery exposed Lenovo PC users to a vulnerability. Superfish said that it was unaware of the security risk that its own software created—a questionable assertion in light of the fact that Komodia holds itself out as an "SSL hijacker." Superfish stated that it has disabled VisualDiscovery "on the server side (i.e., Superfish's search engine . . . ."[75]

72. Superfish's statement—specifically its assertion that the software presents no security risk—has been criticized as "hard to fathom" in that "[t]he certificate that makes the security vulnerability possible clearly carries the Superfish name, was installed as part of the Superfish software, and was produced in collaboration with Komodia, a company Superfish has acknowledged it hired to work on the Lenovo implementation."[76] According to ARS Technica, all the statement establishes is that "Pinhas has trouble owning up to the decisions made by his own company."[77]

---

[72] David Auerbach, *Are Lenovo and Superfish Evil or Incompetent*, Slate (Feb. 24, 2015), http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_the_result_of_evil_or_incompetence.single.html (last visited March 3, 2013).

[73] Dan Goodin, *Superfish Doubles Down, Says HTTPS-busting Adware Poses No Security Risk*, ARS Technica (Feb. 20, 2015), http://arstechnica.com/security/2015/02/superfish-doubles-down-says-https-busting-adware-poses-no-security-risk/ (last visited March 3, 2015).

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

Media and Technology Industry Reaction to the Superfish Scandal

73. Media and technology industry insiders have sharply criticized both Lenovo and Superfish's role in the Superfish scandal.

74. According to the EFF:

- The VisualDiscvoery software Lenovo preloaded onto its PCs is: "horrifically dangerous."[78]
- Superfish's decision to uses man-in-the-middle and fake certificates to inject advertisements "was an amateurish design choice" because it exposes users to serious security risks.[79]
- Lenovo's decision to preload VisualDiscovery onto certain of its PCs was "catastrophically irresponsible and an utter abuse of the trust their customers placed in them."[80]

75. Software engineer and technology writer, David Auerbach opined that "[i]t was ghastly that Lenovo unwittingly preinstalled security-defeating adware/malware" on its laptops and dubbed "the Lenovo-Superfish security hole the biggest tech-customer betrayal in a decade."[81] In giving Lenovo a 5/5 incompetence rating over this scandal and citing the interview Lenovo vice president Mark Cohen gave with InfoWorld, Auerbach noted "Lenovo *knew* Superfish messed with SSL connections *before* it had" surreptitiously loaded it onto customers' computers.[82] But, rather than "dropping Superfish like a rock, which is what you're supposed to do when a software partner compromises your customers' security, it told Superfish to fix it" and then "*didn't bother to check the fix*."[83]

---

[78] *Lenovo is Breaking HTTPS Security on its Recent Laptops*.

[79] *Id.*

[80] *Id.*

[81] *Are Lenovo and Superfish Evil or Incompetent?*

[82] *Id.* (emphasis in original).

[83] *Id.* (emphasis in original).

76. Regarding VisualDiscovery, Auerbach stated that the spyware is an "intrusive form of adware that injects its own results into your searches . . . catastrophically compromis[ing] the security of your entire machine."[84] He concluded that Superfish did not care whether it 'got things right', citing the fact that it "bought a dubious piece of code from Komodia that was *actually marketed* as an 'SSL hijacker.' The words 'SSL hijacker' should give pause to any responsible tech" company.[85] Auerbach concluded that Superfish knew it was compromising users' security because "[a] software company cannot integrate an 'SSL hijacker' into its product without having *some* idea of what it's doing."[86]

77. By choosing to do business with an unscrupulous entity like Superfish, "Lenovo sold its soul to the devil and forgot to get much in return. Homer Simpson would've made a better Faustian bargain."[87] "*Reckless*, *careless*, and *appalling* don't even come close to" describing what Lenovo has done.[88]

78. Technology industry insider Michael Masnick criticized Superfish's method for injecting ads as "astoundingly stupid . . . making it a *massive* security hole that is *insanely dangerous*."[89] The Daily Mail spoke with security analysts that described what Superfish does as "[to] serve intrusive ads, as well as compromise private information such as bank details and passwords."[90] It called this scandal a "horrifically dangerous" and "egregious security failure."[91]

---

[84] *Id.*

[85] *Id.* (emphasis in original).

[86] *Id.* (emphasis in original).

[87] *You Had One Job, Lenovo*.

[88] *Id.* (emphasis in original).

[89] Mike Masnick, *Lenovo in Denial: Insists There's No Security Problem With Superfish—Which Is Very, Very Wrong*, Techdirt, (Feb. 19, 2015) (emphasis in original), https://www.techdirt.com/articles/20150219/10124430071/big-lenono-lenovo-massively-compromises-customers-security-brushes-it-off-as-no-biggie.shtml (last visited March 3, 2015).

[90] Ellie Zolfagharifard, *Are YOU under threat from a Superfish attack? Lenovo PCs May Have Adware—and a 'Horrifically Dangerous' Security Flaw*, DailyMail (Feb. 19, 2015), http://www.dailymail.co.uk/sciencetech/article-2960608/Are-threat-Superfish-attack-Lenovo-PCs-adware-horrifically-dangerous-security-flaw.html (last visited March 3, 2015).

[91] *Id.*

79. Security researcher Marc Rogers concluded that Lenovo's actions were "unbelievably ignorant and reckless."[92] He called this "quite possibly the single worst thing I have seen a manufacturer do to its customer base."[93] "Because this certificate is so weak, anyone can take it's [sic] private key, use the password and sign anything from fake certificates to viruses or malware and your PC will trust it because it is signed by a trusted certificate. . . . I cannot understate how evil this is."[94] According to Rogers, Lenovo's conduct constitutes a breach of trust that jeopardized the security of its customer base:

> We trust our hardware manufacturers to build products that are secure. In this current climate of rising cybercrime, if you can't trust your hardware manufacturer, you are in a very difficult position. That manufacturer has a huge role to play in keeping you safe – from releasing patches to update software when vulnerabilities are found to behaving in a responsible manner with the data the [sic] collect and the privileged access they have to your hardware.[95]

V. PLAINTIFFS' PURCHASES

80. Plaintiff Estrella purchased a Lenovo Yoga 2 Pro in October or November 2014. Plaintiff generally uses her Yoga 2 Pro for a combination of business and personal purposes.

81. Plaintiff Ferezan purchased a Lenovo Yoga 2-11, model 20428 in January 2015. Plaintiff generally uses her Yoga 2-11 for personal purposes.

82. Plaintiff Whittle purchased a Lenovo PC, model G50-70 in October 2014.

83. Plaintiff Woyt purchased two Lenovo PCs, a ThinkPad Yoga 14 and a Yoga 2-11 on December 1, 2014. Plaintiff purchased his Lenovo PCs from Best Buy in Conroe, Texas. Plaintiff paid $1,099.99 for the ThinkPad Yoga 14 and $386.99 for the Yoga 2-11. Plaintiff generally used his ThinkPad Yoga 14 for business purposes and used his Yoga 2-11 for personal purposes.

84. Lenovo preloaded Plaintiffs' PCs with Superfish VisualDiscovery spyware.

85. Had Plaintiffs known that Lenovo had preloaded VisualDiscovery onto their PCs, they would not have elected to purchase such PCs.

---

[92] *Lenovo Installs Adware On Customer Laptops and Compromises ALL SSL.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

VI. CLASS ACTION ALLEGATIONS

86. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and a proposed nationwide class ("Class") initially defined as:

> All persons who purchased Lenovo computers preloaded with Superfish's VisualDiscovery software from August 2014 to present in the United States.

87. Excluded from the proposed class are Lenovo (United States), Inc., Superfish, Inc., their parents, subsidiaries, affiliates and controlled persons, as well as the officers and directors (and their immediate family) of Lenovo (United States, Inc.), their parents, subsidiaries, affiliates and controlled persons. Also excluded is any judicial officer assigned to this case.

88. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4).

89. Numerosity—Fed. R. Civ. P. 23(a)(1). The members of the class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiffs at the present time and can only be ascertained through appropriate discovery, Plaintiffs believe that there are in excess of one million members of the class located throughout the United States. It would be impracticable to join the class members individually.

90. Existence and predominance of common questions of law—Fed. R. Civ. P. 23(a)(2), 23(b)(3). Common questions of law and fact exist as to all members of the class and predominate over any questions solely affecting individual members of the class. Among the many questions of law and fact common to the class are:

(i) whether content the affected Lenovo PC users send to or receive from HTTP or HTTPS websites constitute communications within the meaning of state and federal wiretap laws;

(ii) whether VisualDiscovery intercepts communications "in transit" or "in storage;"

(iii) whether the affected Lenovo PCs constitute a "machine, instrument or contrivance;"

(iv) whether Defendants obtained consent from Plaintiffs and Class members or were otherwise "authorized" to intercept the communications;

(v) whether the affected Lenovo PCs are "protected computers" under the Computer Fraud and Abuse Act;

(vi) Whether Lenovo intentionally preloaded VisualDiscovery onto the affected models of Lenovo PCs;

(vii) Whether Superfish intentionally applied its VisualDiscovery software across both HTTP and HTTPS websites;

(viii) whether the affected Lenovo PCs or Superfish's servers constitute facilities within the meaning of the SCA;

(ix) whether Plaintiffs and Class members had a reasonable expectation of privacy in their communications with encrypted HTTPS websites;

(x) whether Defendants' conduct would be highly offensive to a reasonable person;

(xi) whether Superfish intercepted "content";

(xii) whether Defendants acted "willfully;"

(xiii) whether Defendants violated the California Invasion of Privacy Act, Article I, Section 1 of the California Constitution, the Federal Wiretap Act, the Stored Communications Act, the Computer Fraud and Abuse Act, the California Computer Crime Law, or California's Unfair Competition Law;

(xiv) whether Defendants are liable for trespass to chattels or invasion of privacy; and,

(xv) whether Lenovo acted negligently by preloading the affected Lenovo PCs with VisualDiscovery or by failing to detect the risk presented to consumers by VisualDiscovery.

91. Typicality—Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of the claims of the members of the class. Among other things, Plaintiffs and Class members purchased the affected Lenovo PCs and have been harmed by Defendants' unlawful activities alleged herein.

92. Adequacy—Fed. R. Civ. P. 23(a)(4). Plaintiffs will adequately represent the proposed Class members. They have retained counsel competent and experienced in class actions and internet privacy litigation and intend to pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of class members.

93. Superiority—Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

94. In the alternative, the class may be certified under Rule 23(b)(1), 23(b)(2) or 23(c)(4) because:

(i) The prosecution of separate actions by the individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants;

(ii) The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;

(iii) Defendants acted or refused to act on grounds generally applicable to the class, thereby making appropriate final injunctive relief with respect to the members of the class as a whole; and

(iv) The claims of class members are comprised of common issues that are appropriate for certification under Rule 23(c)(4).

VII. CLAIMS

COUNT ONE
(Against Defendants)

VIOLATION OF CALIFORNIA PENAL CODE §§ 631 AND 637.2
CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")

95. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

96. California Penal Code § 631(a) makes it unlawful, by means of any machine, instrument or contrivance, to purposefully intercept the content of a communication over any "telegraph or telephone wire, line, cable or instrument," or to read or attempt to read or learn the content of any such communications without the consent of all parties to the communication. California Penal Code § 631(a) also makes it unlawful to aid, employ, or conspire with any person doing, permitting, or causing to be done any of these things.

97. Uniform resource locators (URLs), web page get and post commands, emails and other content sent to or received from HTTP and HTTPS websites are communications within the meaning of Section 631.

98. Superfish intercepts, reads, and learns the content of Plaintiffs and Class members communications using machines, instruments or contrivances as defined by the CIPA.

99. Lenovo intentionally preloaded the affected Lenovo PCs with VisualDiscovery spyware in order to intercept the contents of Plaintiffs and Class members electronic communications without consent, including URLs, search terms, emails, and other content.

100. Plaintiffs and Class members did not consent to Superfish's interception and reading of their communications. Alternatively, Plaintiffs and Class members did not consent to Superfish's interception and reading of their communications sent to or received from encrypted HTTPS websites.

101. Plaintiffs and Class members did not consent to Lenovo's preloading of the affected Lenovo PCs with spyware capable of such interception and reading.

102. Superfish is not an intended party to the communications.

103. Superfish is a "person" within the meaning of the CIPA.

104. Lenovo is a "person" within the meaning of the CIPA.

105. Plaintiffs and Class members were and are injured by Superfish's unlawful interception and reading of their communications.

106. Plaintiffs and Class members were and are injured by Lenovo's choice to preload the affected Lenovo PCs with VisualDiscovery because that choice facilitated Superfish's unlawful interception and reading of their communications.

107. Superfish's conduct in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices and operating policies that Superfish developed, implemented and utilized in California which are unlawful and constitute criminal conduct in Superfish's state of residence and principal place of business. Superfish profited from its conduct in the State of California. Superfish also intercepted some of the Class members' communications in California and used at least some devices located in California.

108. As a result of Defendants' violations of Section 631, Plaintiffs and Class members are entitled to relief under Section 637.2, including:

(i) Preliminary and injunctive relief;

(ii) Appropriate declaratory relief;

(iii) Statutory damages of $5,000 per class member; and

(iv) Reasonable attorneys' fees and costs.

COUNT TWO
(Against Defendants)

VIOLATION OF THE CALIFORNIA CONSTITUTION
ARTICLE I, SECTION 1

109. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

110. Article I, Section 1 of the California Constitution provides that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness, and privacy."

111. The California Supreme Court has recognized a private right of action for monetary damages and injunctive relief against non-governmental defendants for violations of the constitutional right to privacy.

112. Plaintiffs and Class members have a legally protected interest in their private communications including in content they send to or receive from websites.

113. Plaintiffs and Class members reasonably expect that their electronic communications are private, and do not expect spyware to intercept them without their consent.

114. Superfish commits an egregious breach of social norms when it intercepts Plaintiffs and Class members' communications without Plaintiffs and Class members' knowledge and consent, and for its own profit.

115. Lenovo commits an egregious breach of social norms when it intentionally preloads spyware capable of such interception of Plaintiffs and Class members' communications without Plaintiffs and Class members' knowledge and consent, and for its own profit.

116. Defendants' acts in violation of the California Constitution occurred in the State of California because those acts resulted from business decisions, practices and operating policies that Superfish developed, implemented and utilized in California which are unlawful and constitute criminal conduct in Superfish's state of residence and principal place of business. Superfish profited from its conduct in the State of California. Lenovo profited from Superfish's conduct in the state of California. Superfish also intercepted, scanned and stored some of the class members' communications in California and used at least some devices located in California.

COUNT THREE
(Against Defendants)

VIOLATION OF THE FEDERAL WIRETAP ACT
TITLE I OF THE ECPA, 18 U.S.C. §§ 2510 *ET SEQ.*

117. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

118. The Wiretap Act prohibits the intentional interception by any person of the content of any wire, oral or electronic communications without the consent of at least one authorized party to the communication. The Wiretap Act also prohibits intentionally procuring other persons to intercept the content of any wire, oral or electronic communications without the consent of at least one authorized party to the communication

119. Superfish and Lenovo are both "persons" within the meaning of the Act.

120. Superfish intercepted the contents of Plaintiffs and Class members' electronic communications without consent, including URLs, search terms, emails, and other content.

121. Lenovo intentionally preloaded the affected Lenovo PCs with VisualDiscovery spyware in order to intercept the contents of Plaintiffs and Class members' electronic communications without consent, including URLs, search terms, emails, and other content.

122. Plaintiffs and Class members were not aware that Defendants were intercepting their electronic communications nor were they aware that VisualDiscovery was preloaded on the affected Lenovo PCs.

123. Plaintiffs and Class members are persons whose electronic communications were intercepted within the meaning of Section 2520.

124. Pursuant to 18 U.S.C. § 2520(a), Plaintiffs and class members are entitled to:

(i) injunctive relief;

(ii) appropriate declaratory relief;

(iii) statutory damages of $100 per day per violation per class member, up to $10,000 per class member;

(iv) costs; and

(v) reasonable attorneys' fees.

COUNT FOUR
(Against Superfish)

VIOLATION OF THE STORED COMMUNICATIONS ACT ("SCA")
TITLE II OF THE ECPA, 18 U.S.C. §§ 2701 *ET, SEQ.*

125. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

126. The Stored Communications Act prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic communications service is provided and thereby obtaining an electronic communication while it is in "electronic storage."

127. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

128. Plaintiffs allege that Superfish intercepts communications while "in transit" and thus in violation of the Wiretap Act. Plaintiffs and Class members assert this SCA claim in the alternative, in the event the Court finds that Superfish intercepts the emails while they are in "storage" rather than "in transit" or holds that Plaintiffs and Class members may assert both a Wiretap Act claim and an SCA claim simultaneously.

129. The affected models of Lenovo PCs are facilities within the meaning of the SCA.

130. Alternatively, Superfish's servers are facilities within the meaning of the SCA.

131. Superfish is a "person" within the meaning of the SCA.

132. Superfish accessed the content of Plaintiffs and Class members' stored communications without authorization or exceeded its authorization from any party to such communications.

133. Pursuant to 18 U.S.C. § 2707(c), Plaintiffs and Class members are entitled to:

(i) minimum statutory damages of $1,000 per person;

(ii) punitive damages;

(iii) costs; and

(iv) reasonable attorneys' fees.

COUNT FIVE
(Against Defendants)

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")
(18 U.S.C. § 1030)

134. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

135. The Consumer Fraud and Abuse Act prohibits persons or entities from obtaining information by intentionally accessing a protected computer without authorization. The Consumer Fraud and Abuse Act specifically prohibits obtaining information from the records of financial institutions. The Consumer Fraud and Abuse Act additionally prohibits knowingly transmitting programs, information, codes, or commands without authorization.

136. Plaintiffs and Class members' affected computers were used in interstate commerce or communication, and were protected computers within the meaning of the CFAA.

137. Superfish intentionally accessed Plaintiffs and Class members' computers without authorization or by exceeding authorized access to such computers, and by obtaining information form such protected computers.

138. Defendants' knowingly caused the transmission of a program, information, code or command to the affected Lenovo PCs and as a result caused a loss to Plaintiffs and Class members during any one-year period of at least $5,000 in the aggregate.

139. Plaintiffs and Class members have also suffered a violation of their privacy rights as a result of Defendants' knowing actions.

140. Defendants have therefore violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

141. Defendants' unlawful access to Plaintiffs and Class members' computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs and Class members' remedies at law are not adequate to compensate for these inflicted threatened injuries, entitling Plaintiffs and Class members to damages and injunctive relief as provided by 18 U.S.S. § 1030(g).

COUNT SIX
(Against Defendants)

VIOLATION OF CALIFORNIA PENAL CODE § 502
THE CALIFORNIA COMPUTER CRIME LAW ("CCCL")

142. Plaintiffs incorporate the above allegations as if fully set forth herein.

143. The CCCL prohibits knowingly and without permission: (a) accessing computers, computer systems, or computer networks in order to defraud or obtain money; (b) accessing and taking data from computers, computer systems, and computer networks; (c) disrupting or causing the disruption of computer services; (d) accessing a computer, computer system, or computer network; (e) providing or assisting in providing a means of such access; (f) introducing a "computer contaminant" into any computer, computer system, or computer network; and, (g) providing or assisting in providing means to access a computer, computer system, or computer network.

144. VisualDiscovery and the software it uses to "hijack" SSL certificates are "computer contaminants" under Cal. Penal Code § 502(b)(10).

145. Defendants accessed, copied, used, made use of, interfered with, and/or altered data belonging to Plaintiffs and Class members: (1) in and from the State of California; and, (2) in the states in which Plaintiffs and Class members are domiciled.

146. Defendants violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, and using Plaintiffs and Class members' personally identifiable information and rendering the affected Lenovo PCs vulnerable to SSL spoofing attacks without a warning from the browser.

147. Defendants' violated Cal. Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs and Class members' computers in order to execute a scheme to defraud consumers by utilizing and profiting from the sale of their private data.

148. Defendants' violated Cal. Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing a means of accessing Plaintiffs and Class members' computer systems and/or computer networks.

149. Defendants violated Cal. Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs and Class members' computer systems and/or computer networks.

150. Defendants violated Cal. Penal Code § 502(8) by knowingly and without permission introducing "computer contaminants" into Plaintiffs and Class members' Lenovo PCs and web sessions—specifically, VisualDiscovery and the SSL hijacking software it utilizes to break into HTTPS websites.

151. As a direct and proximate result of Defendants' unlawful conduct within the meaning of Cal. Penal Code § 502, Defendants have damaged Plaintiffs and Class members in an amount to be proven at trial. Plaintiffs and Class members are additionally entitled to recover reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

152. Plaintiffs and Class members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

153. Plaintiffs and Class members have suffered irreparable harm and injuries from Defendants' violations. The harm will continue unless Defendants are enjoined from further violations of this section. Plaintiffs and Class members have no adequate remedy at law.

154. Plaintiffs and Class members are entitled to punitive or exemplary damages under Cal. Penal Code § 502(e)(4) because Defendants' violations were willful and, upon information and belief, defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

COUNT SEVEN
(Against Defendants)

VIOLATION OF CALIFORNIA BUSINESS AND PROFESSIONAL CODE §§ 17200, *ET SEQ.* THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

155. Plaintiffs incorporate the above allegations as if fully set forth herein.

156. Defendants' acts and practices, as alleged in this complaint, constitute unlawful, unfair and/or fraudulent business practices, in violation of the Unfair Competition Law, Cal. Bus & Prof. Code §§ 17200, et seq.

157. Defendants violated the UCL by knowingly preloading VisualDiscovery without obtaining consent from users of the affected Lenovo PCs or disclosing the ability of such spyware to harvest data from Plaintiffs and Class members' encrypted web sessions. Superfish intentionally used software that held itself out as a "SSL hijacker" in its VisualDiscovery program and therefore knew or should have known that VisualDiscovery would invade Plaintiffs and Class members' privacy. Lenovo failed to implement adequate mechanisms for quality control of the bloatware that it preloaded onto the affected Lenovo PCs and failed to disclose to its consumers that such bloatware would negatively affect performance, and that VisualDiscovery would invade Plaintiffs and Class members' privacy and expose them to a substantial risk of cyber-attack in the process. Defendants each profited by including VisualDiscovery on the affected Lenovo PCs.

158. Defendants' conduct constitutes unlawful, unfair and fraudulent business acts and practices, and as a proximate result of those business acts and practices, Plaintiffs and Class members have suffered harm and lost money and/or property.

159. By engaging in the business acts and practices described herein, Defendants have committed one or more acts of unfair competition within the meaning of the UCL.

160. Defendants' business acts and practices are "unfair" and "unlawful" within the meaning of the UCL because such business acts and practices violate CIPA, Article I, Section I of the California Constitution, the Federal Wiretap Act, the SCA, the CFAA, and the CCCL. Plaintiffs and Class members were damaged and lost money and/or property as a result.

161. Defendants engaged in fraudulent business practices by engaging in conduct that was and is likely to deceive a reasonable purchaser of the affected Lenovo PCs.

162. As a direct and proximate result of Defendants' unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiffs and Class members have suffered injury in fact and lost money or property, in that they purchased affected Lenovo PCs that they otherwise would not have pursuant to misrepresentations that caused such PCs to: (1) perform more poorly than they would have absent installation of the bloatware; (2) invade Plaintiffs and Class members' privacy; and, (3) expose Plaintiffs and Class members to a substantial and actual risk of cyber-attack. Meanwhile, Defendants have generated more revenue connected to Lenovo's sale of a substantial number of PCs with VisualDiscovery preloaded onto them than they otherwise would have.

163. Plaintiffs and Class members are entitled to equitable relief, including restitutionary disgorgement of all profits accruing to Defendants because of their unlawful, unfair, fraudulent, and deceptive practices, attorney's fees and costs, declaratory relief, and a permanent injunction enjoining Defendants from their unlawful, unfair, fraudulent, and deceitful activity.

COUNT EIGHT
(Against Defendants)

TRESPASS TO CHATTELS

164. Plaintiffs incorporate the above allegations as if fully set forth herein.

165. Defendants, intentionally and without consent or other legal justification, tracked, intercepted and scanned Plaintiffs and Class members' internet activity.

166. Defendants, intentionally and without consent or other legal justification, placed malicious spyware on Plaintiffs and Class members' PCs which exposed the affected Lenovo PCs to a substantial risk of cyber-attack via HTTPS spoofing.

167. Defendants' intentional and unjustified preloading of malicious spyware onto Plaintiffs and Class members' PCs and interception, scanning, and alteration of Plaintiffs and Class members' communications interferes with Plaintiffs and Class members' use of the affected Lenovo PCs. Alternatively, Defendants' conduct damaged the affected Lenovo PCs by causing them to perform more poorly than they would have absent the VisualDiscovery spyware.

168. Plaintiffs and Class members were harmed by Defendants' conduct and Defendants' conduct was a substantial factor in causing such harm.

COUNT NINE
(Against Defendants)

INVASION OF PRIVACY

169. Plaintiffs incorporate each and every allegation as if fully set forth herein.

170. Plaintiffs had an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential personally identifiable information; and, (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet websites—including encrypted HTTPS websites—without having the content they sent to or received from such sites intercepted, scanned, and transmitted to Defendants without their knowledge or consent.

171. Plaintiffs had a reasonable expectation that their personally identifiable information and other sensitive information—like banking and email login credentials and the content on such websites—would remain confidential and that Defendants would not install and deploy spyware on the affected Lenovo PCs that would enable tracking, interception, and scanning of content.

172. This invasion of privacy is sufficiently serious in nature, scope, and impact.

173. This invasion of privacy constitutes an egregious breach of the social norms underlying the privacy right.

COUNT TEN
(Against Lenovo)

NEGLIGENCE

174. Plaintiffs incorporate each and every allegation as if fully set forth herein.

175. Lenovo owed Plaintiffs and Class members a duty to provide accurate information as to the bloatware it preloaded onto the affected Lenovo PCs, to protect against any dangers to its customer base presented by such bloatware, and to exercise adequate quality control over such bloatware prior to shipping the affected PCs for sale.

176. A finding that Lenovo owed a duty to Plaintiffs and Class members would not impose a significant burden on Lenovo. Lenovo has the means to accurately guard against preloading malicious and dangerous spyware on its PCs by ensuring that adequate quality control mechanisms are in place and followed by affected employees. The cost borne by Lenovo for these efforts is insignificant in light of the dangers posed to Plaintiffs and Class members by Lenovo's failure to take such steps toward ensuring its substantial base of PC users are apprised of the presence and capability of the spyware, and ensuring that such spyware does not illegally scan content sent to or received from encrypted HTTPS websites Lenovo chooses to preload onto the PCs they purchase.

177. As recently confirmed by Lenovo, it was unaware of the Security danger presented by VisualDiscovery—an ad-injector that relies on a self-described SSL hijacker to do its job—until late February 2015. By failing to adequately test VisualDiscovery before preloading it onto the affected Lenovo PCs and shipping them to the public, Lenovo departed from the reasonable standard of care and breached its duties to Plaintiffs and other purchasers of the affected Lenovo PCs.

178. As a direct, reasonably foreseeable, and proximate result of Lenovo's failure to exercise reasonable care, provide accurate information as to the its preloaded bloatware, and exercise adequate quality control over such bloatware, Plaintiffs and Class members have suffered damages.

179. Plaintiffs and Class members could not through the exercise of reasonable diligence have prevented the damages caused by Lenovo's negligence. Neither Plaintiffs nor other Class members contributed to Lenovo's decision to preload VisualDiscovery onto the affected Lenovo PCs.

COUNT ELEVEN
(Against Defendants)

DECLARATORY RELIEF
28 U.S.C. § 2201

180. Plaintiffs incorporate each and every allegation above as if fully set forth herein

181. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiffs and Defendants for which Plaintiffs desire a declaration of rights.

182. Plaintiffs contend and Defendants dispute that Defendants' acts, practices and conduct violate the CIPA and the federal Wiretap Act or, in the alternative, the Stored Communications Act, as alleged herein.

183. Plaintiffs, on behalf themselves and the class, are entitled to a declaration that Defendants illegally intercepted and scanned their electronic communications, improperly accessed the affected Lenovo PCs, violated the federal and state statutes and laws alleged herein, and are entitled to injunctive relief to enforce the Court's declaration.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

(a) That the Court enter an order certifying the class, appointing Plaintiffs as representatives of the class, and appointing Plaintiffs' counsel as class counsel;

(b) That the Court enter judgment against Defendants for the causes of action alleged against them;

(c) That Plaintiffs be awarded statutory and common law damages as provided by California and federal law, plus interest, as well as litigation costs reasonably incurred and attorneys' fees;

(d) That the Court order the disgorgement of all revenues unjustly earned by Defendants for selling or otherwise trading on the content of communications Superfish improperly intercepted and scanned;

(e) That the Court award appropriate injunctive relief, including requiring Defendants to cease intercepting Plaintiffs and Class members' communications, and permanently delete all data they have collected and stored from or related to Class members; and

(f) That the Court enter a declaratory judgment that the conduct complained of in this Complaint is unlawful and violates state and federal law.

IX. JURY DEMAND

Plaintiffs, individually and for the Class they seek to represent, demand trial by jury on each and every triable issue.

DATED: March 5, 2015

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Adam E. Polk*
Adam E. Polk

Daniel C. Girard
Adam E. Polk
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

NICHOLS KASTER, PLLP
E. Michelle Drake
Megan D. Yelle
4600 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Phone: (612) 256-3200
Fax: (612) 338-4878

Counsel for Individual and Representative Plaintiffs Rhonda Estrella, Sonia Ferezan, Alan Woyt, and John Whittle